IN THE UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF GEORGIA ATLANTA DIVISION

DONNA CURLING, et al., **Plaintiffs,** **v.** **BRAD RAFFENSPERGER, et al.,** **Defendants.**	**Civil Action No.: 1:17-cv-2989-AT**

DECLARATION OF KEVIN SKOGLUND

Pursuant to 28 U.S.C. § 1746, I, KEVIN SKOGLUND, declare under penalty of perjury that the following is true and correct:

1. This declaration supplements my declarations previously submitted in this case, and I incorporate my previous declarations as if fully stated herein.

2. The Coalition Plaintiffs asked me to advise on the propriety and security risks of lifting the seal on the redacted version of the report, "Security Analysis of Georgia's ImageCast X Ballot Marking Devices," by Dr. Halderman and Dr. Springall ("ICX Report").

3. It is my opinion that the seal on the redacted ICX Report can be lifted and the public *should* be permitted to learn its contents.

4. I read the unredacted ICX Report in July 2021. I reviewed the redacted report around November 2021 and again this month. My opinion at the time and

still today is that the redacted ICX Report is suitable for public release. It describes several serious vulnerabilities which increase security risks but which remain unknown to key stakeholders, such as state and county election officials both inside and outside of Georgia. The unredacted text provides sufficient detail for these stakeholders to understand and manage the risks. The redacted text hides technical details which are not useful to stakeholders but which might be useful to adversaries.

5. Disclosing vulnerabilities responsibly is not a new challenge. Coordinated Vulnerability Disclosure ("CVD") has become a common practice for disclosing security research. CVD balances several equities while improving security. CVD programs allow a vendor to validate a report and develop mitigations over a set period of time before the vulnerability is disclosed to the public. However, CVD does not grant vendors permission to be slow or unresponsive because the time period until public disclosure is reasonable but limited. From the point of view of the users whose security is a risk, a finite delay strikes a good balance between immediate disclosure and unlimited procrastination.

6. It is common for CVD programs to allow a vendor 90 days to validate a report and to develop mitigations before the vulnerability is disclosed to the public. It is my opinion that election systems require more time in most cases—due to the need for federal and state certification and the difficulty of upgrading

systems during the weeks when an election is underway—but 180 days is sufficient.

7. The Court has observed the feasibility of developing, certifying, and installing certain software changes quickly. At the end of September 2020, the Secretary of State identified an issue with the two-column display of candidates on the ImageCast X BMDs. In just 14 days, Dominion created a software update, got it reviewed by a Voting System Test Lab, and received federal and state certification, while the Secretary of State oversaw its distribution and installation in over 30,000 BMDs. Processes can move quickly when motivated.

8. It has been 683 days since the ICX Report was written on July 1, 2021. It is my understanding that the Secretary of State and Dominion read the unredacted report soon after it was written. It is also my understanding that Dominion shared the unredacted report with a cybersecurity team at MITRE, and that the Secretary of State retains Fortalice as a cybersecurity advisor. They have had more than enough time to assess the vulnerabilities and to mitigate the increased risks. Any failure to act after almost two years is their responsibility. (CVD does not allow unlimited procrastination because unaddressed issues are harmful to security.)

9. Dominion may have mitigated vulnerabilities in a subsequent software version. Dominion submitted its Democracy Suite 5.17 software ("DS 5.17") for EAC certification on October 4, 2022 and received approval on March 16, 2023. DS 5.17 includes software changes that appear to be related to the ICX Report. I

do not know if DS 5.17 adequately addresses all of the vulnerabilities in the ICX Report, but I have no doubt Dominion has had sufficient opportunity to address them.

10. Many security-sensitive actions can be evaluated by whether they help the "defenders" or the "attackers" more. Lifting the seal on the redacted ICX Report will benefit other jurisdictions which have not had an opportunity to evaluate it and consider mitigations. For example, reading it may hasten adoption of the DS 5.17 software and generate substantive conversations about remaining areas of concern. Without that knowledge, some jurisdictions may not understand or fully appreciate the risks and may remain more vulnerable to malfeasance than they realize. Defenders get no benefit if the redacted ICX Report remains under seal.

11. I do not think lifting the seal on the redacted ICX Report will benefit attackers significantly. Adversaries will learn non-technical details about the vulnerabilities, but not the technical recipes necessary to exploit them. (Accordingly, I do not favor releasing the *unredacted* ICX Report to the public.) Adversaries with modest technical skills would not have enough information to abuse it. Adversaries with advanced skills can discover the same vulnerabilities without the technical details. Dr. Halderman and Dr. Springall spent approximately 12 person-weeks on their analysis. A well-resourced adversary could do the same work in days. These conclusions are unaffected by the

unregulated distribution of election software from Coffee County and elsewhere. Unlike the defenders, attackers will benefit if the redacted ICX Report remains under seal because more defenders may remain under-protected and even adversaries with no technical skills can traffic in disinformation about what the sealed report contains.

12. I conclude that releasing the redacted ICX Report is of much greater benefit to the defenders than to the attackers.

13. The Court does not need to manage a CVD program or shoulder responsibility for the impact of vulnerability disclosures. Dominion and the Secretary of State have the means and expertise to address vulnerability reports. Other jurisdictions also have the means and expertise, provided they gain access to the redacted ICX Report.

14. It is for these reasons that I favor lifting the seal on the redacted ICX Report.

Executed on this date, May 15, 2023.

Kevin Skoglund